

CLAIMS

- 1 1. An apparatus for transmitting a file through a network,
2 comprising:
3 a file-splitting processor that splits the file into a
4 plurality of message segments and addresses the
5 plurality of message segments to a plurality of
6 addresses assigned to a receiving host; and
7 a message segment transmitter for transmitting the
8 plurality of message segments to the receiving host.
- 1 2. The apparatus of claim 1 wherein the file splitting
2 processor comprises a file converter that converts the
3 file into N message segments that enable reassembly of
4 the file from a subset of any K of the message segments,
5 wherein N and K are positive integers, and $N > K > 1$.
- 1 3. The apparatus of claim 1 wherein the file-splitting
2 processor further assigns a plurality of source addresses
3 to the plurality of message segments to impede
4 unauthorized attempts to observe the true source of a
5 transmitted file.
- 1 4. The apparatus of claim 1 further comprising a message
2 segment monitor for detecting non-receipt of at least one
3 of a second plurality of message segments transmitted to
4 the apparatus.
- 1 5. The apparatus of claim 1 further comprising an address
2 allocator for assigning and reassigning N addresses to
3 the receiving host.
- 1 6. An apparatus for transmitting a file through a network,
2 comprising:
3 a file-splitting processor that splits the file into a
4 plurality of message segments and assigns a plurality
5 of source addresses to the plurality of message
6 segments to disguise the origin of the file; and

- 7 a message segment transmitter for transmitting the
8 plurality of message segments to a receiving host.
- 1 7. The apparatus of claim 6 wherein the file splitting
2 processor further addresses the plurality of message
3 segments to a plurality of addresses assigned to the
4 receiving host.
- 1 8. A method of secure transmission of a file through a
2 network, comprising:
3 (a) splitting the file into a plurality of message
4 segments;
5 (b) addressing the plurality of message segments to a
6 plurality of addresses assigned to a receiving host;
7 and
8 (c) transmitting the plurality of message segments to the
9 receiving host.
- 1 9. The method of claim 8 wherein addressing comprises
2 addressing the plurality of message segments in one-to-
3 one correspondence to at least a portion of the plurality
4 of addresses.
- 1 10. The method claim 8 wherein splitting the file comprises
2 converting the file into N message segments that enable
3 reassembly of the file from a subset of any K of the
4 message segments, where N and K are positive integers,
5 and $N > K > 1$.
- 1 11. The method of claim 10 further comprising (d) assigning
2 N addresses to the receiving host, and wherein the step
3 of addressing comprises addressing the N message segments
4 to the N addresses assigned to the receiving host.
- 1 12. The method of claim 11 further comprising causing the
2 receiving host to cease receiving messages via at least

3 one address upon detection of an attack on the at least
4 one address.

1 13. The method of claim 12 wherein the receiving host is
2 permitted to cease receiving messages via no more than
3 (N-K) addresses, thereby ensuring reassembly of the file
4 by the host.

1 14. The method of claim 11 further comprising: (e) causing
2 the receiving host to split a reassembled file into N
3 message segments; and (f) causing the receiving host to
4 transmit the N message segments from the N addresses.

1 15. The method of claim 8 further comprising (d) causing
2 the receiving host to retransmit the plurality of message
3 segments.

1 16. The method of claim 15 wherein the step of causing the
2 receiving host to retransmit comprises causing the
3 receiving host to retransmit the plurality of message
4 segments to at least two of a plurality of hosts to relay
5 the plurality of message segments along more than one
6 path through the network.

1 17. The method of claim 8 further comprising: (d) selecting
2 as a virtual network a plurality of hosts that includes
3 the receiving host; and (e) assigning each one of the
4 plurality of hosts to one of a plurality of domains, and
5 wherein the step of transmitting comprises permitting
6 each one of the plurality of message segments to travel
7 to the receiving host only via relays between host pairs,
8 each one of the host pairs selected from one of a same
9 domain and a neighboring domain.

1 18. The method of claim 8 further comprising (d) assigning
2 a plurality of source addresses to the plurality of
3 message segments to impede unauthorized attempts to

4 observe a true source of a transmitted file.

1 19. The method of claim 8 further comprising causing the
2 receiving host to: receive at least a portion of the
3 plurality of message segments; reassemble the file from
4 the received message segments; split the reassembled file
5 into a second plurality of message segments; and transmit
6 the second plurality of message segments.

1 20. The method of claim 8 wherein (c) transmitting
2 comprises transmitting the plurality of message segments
3 to one of an intermediate host and a destination.

1 21. The method of claim 8 wherein (c) transmitting
2 comprises transmitting from one of a source and an
3 intermediate host.

1 22. The method of claim 8 further comprising (d) causing
2 the receiving host to monitor non-receipt of at least one
3 of the plurality of message segments to detect tampering
4 with message segment transmission.

1 23. The method of claim 8 further comprising: (d) assigning
2 N addresses to the receiving host; and (e) repeatedly
3 changing at least a portion of the N addresses.

1 24. The method of claim 10 further comprising (d)
2 repeatedly changing at least a portion of the addresses
3 assigned to the receiving host while leaving at least K
4 of the addresses unchanged, and (e) notifying at least a
5 portion of the network of the changed addresses, and
6 wherein the step of addressing comprises addressing the
7 plurality of message segments to at least the K unchanged
8 addresses to permit continuous receipt of messages by the
9 receiving host.

1 25. The method of claim 8 further comprising: (d) causing a

2 sending host to add status information concerning itself
3 to the message segment; and (e) causing the receiving
4 host to interpret the status information to detect
5 tampering with message segment transmission.

1 26. The method of claim 8 further comprising (d) encoding
2 the file to produce an encoded bit file having encoded
3 bits, and (e) scrambling the encoded bits, and wherein
4 the step of splitting the file splits the encoded bit
5 file.

1 27. A method of secure transmission of a file through a
2 network, comprising:

- 3 (a) splitting the file into a plurality of message
4 segments;
5 (b) assigning a plurality of source addresses to the
6 plurality of message segments to disguise the origin
7 of the file; and
8 (c) transmitting the plurality of message segments.

1 28. The method of claim 27 further comprising (d)
2 addressing the plurality of message segments to a
3 plurality of addresses assigned to a receiving host.

1 29. A method of secure transmission of a message through a
2 network, comprising:

- 3 (a) splitting the file into a plurality of message
4 segments, each message segment comprising a
5 destination specifier, protocol information and
6 message data, the protocol information and message
7 data being encrypted;
8 (b) causing a message segment to be received by a
9 receiving host;
10 (c) causing the receiving host to decrypt the routing

11 information to determine a downstream destination
12 host;
13 (d) causing the receiving host to encrypt the routing
14 information and message data in accordance with an
15 encryption protocol accessible to the destination
16 host, and to transmit the thus-encrypted message
17 segment to the destination host; and
18 (e) repeating steps (a)-(d) for other message segments to
19 facilitate recovery of the message by an ultimate
20 destination host.

1 30. The method of claim 29 wherein the message segment has
2 a length, and further comprising causing the receiving
3 host to alter the length.

1 31. The method of claim 29 further comprising causing the
2 receiving host to negotiate with the destination host to
3 determine the encryption protocol.

1 32. The method of claim 29 further comprising causing the
2 receiving host to add status information concerning
3 itself to the message segment, and causing the receiving
4 host to interpret the status information to detect
5 tampering with message segment transmission.

1 33. A method of defining and operating a network topology
2 to camouflage network traffic patterns and volume, the
3 network comprising a plurality of hosts, the method
4 comprising:

5 (a) assigning each one of the plurality of hosts to one
6 of a plurality of domains;

7 (b) permitting message transmission from each host to
8 hosts within the domain of the host or a domain that
9 neighbors the domain of the host, thereby defining
10 multiple redundant relay paths among hosts; and

11 (c) distributing traffic across the network, thereby
12 camouflaging message sources and destinations.

1 34. The method of claim 33 further comprising (d)
2 reassigning at least one of the plurality of hosts to a
3 different one of the plurality of domains, thereby
4 changing network traffic patterns.

1 35. The method of claim 33 further comprising (d) assigning
2 a plurality of addresses to each one of the plurality of
3 hosts; reassigning the plurality of addresses from a pool
4 of addresses; and notifying the plurality of hosts of the
5 reassigned plurality of addresses.

1 36. The method of claim 35 wherein the step of reassigning
2 comprises reassigning only a portion of the plurality of
3 addresses at any one time to permit use of a remaining
4 unreassigned portion of the plurality of addresses while
5 notifying the plurality of hosts of the reassigned
6 plurality of addresses.